# APPLICATION FOR UNITED STATES PATENT

## EFFICIENT RANDOM NUMBER GENERATION FOR COMMUNICATION SYSTEMS

By Inventors:

Subramanian Meiyappan,
a citizen of India residing at
1221 Altissimo Place
San Jose, CA 95131

Assignee:     Cisco Technology, Inc.
              (A California CORPORATION)
              170 W. Tasman Drive
              San Jose, CA 95134

Entity:       Large


Ritter, Lang & Kaplan LLP
12930 Saratoga Ave., Suite D1
Saratoga, CA 95070
(408) 446-8690

# EFFICIENT RANDOM NUMBER GENERATION FOR COMMUNICATION SYSTEMS

5        ## BACKGROUND OF THE INVENTION

The present invention relates to the generation of random numbers and more particularly to the generation of random numbers in a communication system.

With the ongoing development of the Internet for both commercial transactions

10   and communication of private information, it has become increasingly necessary to encrypt certain Internet information and also to authenticate users and transactions. Protocols employed for authentication and protection of private information typically rely on cryptographic techniques. For example, the IPSEC protocol is used to protect information transported across virtual private networks that facilitate secure private

15   networking over the public Internet. The cryptographic techniques underlying such secure protocols require generation of random numbers to generate encryption and decryption keys that assure secure operation. The security achieved depends on generation of truly random numbers whose values cannot be predicted by those seeking to compromise security.

20        Generating truly random numbers is a non-trivial task. To generate a single truly random number in software may require millions of clock cycles. To accomplish this without severely impacting other processing, a separate hardware accelerator is often

used to offload the main processor, adding expense and complexity.  Another solution is

to substitute a significantly more powerful main processor, also adding expense.

5     There are other techniques that rely only on hardware to generate truly random

numbers.  Typically, the hardware computation of a random number begins by generating

a seed that is obtained by monitoring a randomly varying parameter of a solid state

device or other electronic component.  For example, one may monitor the seek times of

disk drives, thermal noise of a resistor, clock jitter in a phase locked loop, an XOR'ed

combination of oscillator outputs, radioactive decay times, etc.  These techniques require

10    relatively expensive customized hardware.  For example, monitoring thermal noise of a

resistor requires both a specialized resistor and a zener diode.

What is needed are systems and methods for random number generation that

require a minimum of specialized hardware and additional cost, and that can be readily

applied to secure communications.

15

# SUMMARY OF THE INVENTION

According to one embodiment of the present invention, truly random numbers are generated with a minimum of extra hardware by taking advantage of the noise inherent in

5    a communication channel. Random numbers can thus be generated without specialized manufacturing requirements and can be incorporated into conventional integrated circuits with minimal additional logic. The random number generation technique offloads the processor from performing extensive random number generation calculations without the use of a hardware accelerator. This random number generation technique may find

10    application in any network device that participates in a virtual private network or is used to implement secure electronic commerce.

According to one aspect of the present invention, a method for generating a random value includes: monitoring a signal obtained from a communication channel where the signal includes additive noise, sampling the signal to generate a random value,

15    and storing the random value.

A further understanding of the nature and advantages of the inventions herein may be realized by reference to the remaining portions of the specification and the attached drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of random number generation system according to one embodiment of the present invention.

5      Fig. 2 is a flow chart describing operation of the random generation system of Fig. 1.

# DESCRIPTION OF SPECIFIC EMBODIMENTS

5      The present invention will be described in the context of a communication system where information is transmitted over a communication channel by modulating the signal. At the receiver of the communication channel, the modulation signal is received but Additive White Gaussian Noise (AWGN) is also received superimposed on the modulated signal. The AWGN is for most purposes an impairment to the performance of

10     the communication system making it more difficult for the receiver to determine exactly what data has been transmitted. However, according to the present invention, this additive noise is exploited to advantage. The noise is used as the basis for generating a random number that can then support cryptographic activities such as the generation of secure keys. This supports higher-level protocols for authentication and encryption.

15     Examples of communication systems where this additive noise may be exploited include a wireless communication network, a data over cable network, a DSL network, etc. Such networks are often used to implement user access to the Internet at the physical layer. For these networks, the transmission medium, whether it be the airwaves, coaxial cable, twisted pair, etc., adds noise to the propagated signal incident at the receiver.

20     Fig. 1 depicts a random number generation system according to one embodiment of the present invention. Fig. 1 depicts a random number generation system in the context of a communication system that exploits a wireless communication channel. A

random number generation system of the present invention can, however, exploit the additive noise provided by any type of communication channel.

An antenna 102 picks up a modulated signal from the airwaves. The modulated signal is at a frequency referred to as the radio frequency (RF). An analog receiver system 104 receives, amplifies, and filters the RF modulated signal. Analog receiver system 104 also converts the RF signal to an intermediate frequency (IF) to form an IF modulated signal. The IF signal is converted to baseband and sampled and digitized by an analog to digital converter 106. Antenna 102, analog receiver system 104 and analog to digital converter 106 are all components that would be included even without the implementation of the random number generation techniques of the present invention.

The output of analog to digital converter 106 is a digital representation of the transmitted modulated signal plus the noise added by the wireless communication channel. The remaining discussion of random number generation will also refer to a flow chart, Fig. 2.

At step 202, analog to digital converter 106 obtains an N-bit digital sample. The samples are obtained at intervals determined by the design of the communication system. At step 204, a bit reordering block 108 psuedo-randomly scrambles the parallel outputs of analog to digital converter 106. This scrambling is performed separately for each N-bit sample output by converter 106. In one embodiment, this reordering is based on a random N-bit number generated by a linear feedback shift register (LFSR) as known in the art (see citation below). For example, each bit of the N-bit number may be fed to

each of N multiplexers. The select signal for the multiplexers is derived from the LFSR output bits such that each multiplexer outputs a different bit of the N-bit sample output. This LFSR (not shown) can itself be initialized using a sample from analog to digital converter 106.

Not every N bit sample is used in generating random numbers. At step 206, a sampling switch 110 samples the output of bit reordering block 108. Sampling switch 110 samples during periods when its sampling input line is active and does not sample when its sampling input is inactive. Sampling switch 110 may be implemented by a simple FET. The sampling input to sampling switch 110 is provided by the output of a linear feedback shift register 112. The internal structure of linear feedback shift register 112 is known in the art. Further details of linear feedback shift register operation are described in Schneier, Applied Cryptography, (2$^{nd}$ Ed. 1996), pp. 372-378, the contents of this entire volume being incorporated herein by reference for all purposes.

The effect of reordering block 108 and sampling switch 110 is to remove the non-random structure of the transmitted signal and therefore isolate the noise component. The output of sampling switch 110 is also N bits wide and is periodically clocked into a random number storage register 114 at a step 208.

Random numbers will be clocked into register 114 repeatedly and may be recalled for use as needed. Thus, at step 210, the random number in random number storage register 114 may be recalled for use in, e.g., generating a cryptographic key. One example of an application that would make use of this random number is the well-known

IPSEC protocol described in Kent, et al., Request for Comments 2401 published in November 1998 by the Internet Engineering Task Force, the contents are which herein incorporated by reference in their entirety for all purposes.

5       In an alternative embodiment, optimized for use in applications where power consumption is critical such as portable applications, the beginning of a secure session necessitating random number generation activates switch 110 and permits clocking by linear feedback shift register 112. Otherwise, these components (and also bit reordering block 108) are kept off to save power. Once the session begins, the secure application

10      can read random numbers from random number storage register 114 as needed.

The systems and techniques described above achieve random number generation while adding minimal hardware to a communication system. Antenna 102, analog receiver system 104, and analog to digital converter 106 are typically already included in any digital communication system and need not be modified to support random number

15      generation. Assume a 12 bit wide output for converter 106 and a 12 bit number stored in random number storage register 114. Bit reordering block 108 may be implemented in as few as 100 gates. Sampling switch 110 can be a single FET, linear feedback shift register 112 can be implemented in as few as 50 gates, and random number storage register 114 may require as few as 100 gates. Thus, the entire random number capability is added

20      using only approximately 250 gates.

These gates can readily be added to a VLSI integrated circuit that is typically included in the digital communication system for the purpose of implementing signal

processing algorithms. The low cost and simple implementation thus achieved offers a significant advantage over random number generation systems that rely on an additional processor, use of a more powerful digital processor than would be otherwise necessary

5    for digital communications, or specialized parts such as zener diodes, etc.

It is understood that the examples and embodiments described herein are for illustrative purposes only and that various modifications or changes in light thereof will be suggested to persons skilled in the art and are to be included in the spirit and purview of this application and the scope of the appended claims and their full scope of

10    equivalents. Bit reordering block 108, sampling switch 110, and linear feedback shift register 112 represent only one example of a monitoring circuit that monitors the signal received via the communications channel and generates a random number based on this signal.